

Management Informatika Telekomunikace

# Důvěryhodný dokument

**ICT seminář „GDPR, eIDAS, ZoKB. Nové legislativní povinnosti organizací – a co s tím?“**

Autor prezentace: Martin Hapl  
Kontakt: [mhapl@mit-consulting.cz](mailto:mhapl@mit-consulting.cz)  
Datum: 12. 9 2017

# 1 Důvěryhodný dokument

## Co to je ?

Důvěryhodný dokument je dokument, kterému věřím.

Proč mu věřím?

- znám původ dokumentu
- věřím, že obsah je autentický „pravý“

Zatím žádná česká právní norma jednoznačně nedefinuje co to vlastně důvěryhodné dokumenty jsou.

## 2 Důvěryhodný dokument

### Legislativní rámec

Zákon č. 499/2004 o archivnictví a spisové službě

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 – eIDAS

Zákon č. 297/2016 Sb. ze dne 24. srpna 2016, o službách vytvářejících důvěru pro elektronické transakce

Zákon č. 298/2016 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce

## 3 Definice pojmů

### Dokument, Digitální dokument

Zákon č. 499/2004 o archivnictví a spisové službě

§ 2 Vymezení pojmů:

e) dokumentem je každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či **digitální**, která byla vytvořena původcem nebo byla původci doručena

§ 69a Zvláštní ustanovení o dokumentech v **digitální** podobě

~~(5) Neprokáže-li se opak, dokument v digitální podobě se považuje za pravý,.....~~

Byl zrušen zákonem č. 298/2016 Sb.

### Budování důvěry v elektronických transakcích

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014  
ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro  
elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES

V důvodové zprávě zmiňuje mimo jiné:

Budování **důvěryhodnosti** on-line prostředí ...

Toto nařízení má zvýšit **důvěryhodnost** elektronických transakcí ...

Definuje služby vytvářející **důvěru**.

### Elektronický dokument

Článek 3 Definice 35):

„elektronickým dokumentem“ se rozumí jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka.

### Právní účinky elektronických dokumentů

Článek 46

Elektronickému dokumentu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu.

## 6 eIDAS

### Elektronický podpis

„elektronickým podpisem“ se rozumí data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání;

„zaručeným elektronickým podpisem“ elektronický podpis, který splňuje požadavky stanovené v článku 26 „*Požadavky na zaručené elektronické podpisy*“;

„kvalifikovaným elektronickým podpisem“ se rozumí zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy;

„podepisující osobou“ se rozumí fyzická osoba, která vytváří elektronický podpis;

### Právní účinky elektronických podpisů

Článek 25 Právní účinky elektronických podpisů

**Elektronickému podpisu** nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo **že nesplňuje požadavky na kvalifikované elektronické podpisy.**

Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu.



### Podpisování elektronických dokumentů

ZÁKON 297/2016 Sb. ze dne 24. srpna 2016, o službách vytvářejících důvěru pro elektronické transakce

#### **Podpisování dokumentů (§ 5, § 6, § 7)**

- kvalifikovaný elektronický podpis - pokud právně jedná veřejnoprávní původce (stát),
- uznávaný elektronický podpis - pokud právně jedná občan / firma vůči státu,
- jakýkoli typ podpisu - v ostatních případech.

#### **Pečetění dokumentu (§ 8, § 9, § 10)**

- kvalifikovaná elektronická pečeť - pokud právně jedná veřejnoprávní původce (stát),
- uznávaná elektronická pečeť - pokud právně jedná právnická osoba vůči státu.

#### **Použití kvalifikovaného elektronického časového razítka (§ 11)**

- k pečetí nebo podpisu připojí veřejnoprávní původce.

## 9 Elektronický dokument

### Formáty dokumentů pro podpisy

ETSI – European Telecommunications Standard Institute

AdES – standardy rozšířeného elektronického podpisu

ETSI TS 103171 – XAdES

ETSI TS 103172 – PAdES

ETSI TS 103173 – CAdES

ETSI TS 103174 – ASiC

CAdES, PAdES a XAdES – jsou referenčními formáty (rozhodnutí Evropské komise 2011/130/EU).

## 10 Elektronický dokument

### Ověřování platnosti elektronických podpisů a pečeti

MV ČR vydalo dne 24.10.2016 „Metodický návod pro ověřování platnosti uznávaných elektronických podpisů a elektronických pečeti.“

Co je k ověření podpisu potřeba?

- Určit časový okamžik kdy podpis prokazatelně existoval.
- TrustServiceStatusList (TSL) a provést kontrolu zda certifikát byl vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru.
- Získat seznam zneplatněných certifikátů (CRL) nebo, protokol o stavu certifikátu (OCSP) a to pro všechny certifikáty v certifikační cestě posuzovaného certifikátu.

Name	Ext
[..]	
TSL_CZ	pdf
TSL_CZ	xtsl
rca15_rsa	crl
2qca16_rsa	crl
rca15_rsa	cer
2qca16_rsa	cer
e-ucet.o2.cz	cer
Vyúčtování_2016_11-0709142526	pdf

## 11 Elektronický dokument

### Uložení elektronických dokumentů

- Není podstatné jak je elektronický dokument fyzicky uložen.
- Při **dlouhodobém uložení** elektronických dokumentů s podpisem založeným na kvalifikovaném certifikátu je potřeba řešit problém **omezené platnosti** certifikátu.

## 12 Elektronický dokument

### Důvěryhodnost elektronických dokumentů v čase

Prodloužení platností podpisu pomocí časového razítka.

Omezená platnost časového razítka, nutnost přerazítkování.

Prodloužení platnosti CRL, OCSP, TSL, cert.

## 13 Elektronický dokument

### Uložení digitálních dokumentů a prostředků k ověření podpisů

Sdružení dokumentu a prostředku potřebných k ověření podpisů do balíčků

- Vše potřebné v jednom souboru.
- Jedno časové razítko za dokument.

### XAdES

- Sdružení více dokumentů včetně prostředků pro ověření bezpečnostních prvků do jednoho balíku.
- Samotný dokument nemusí být obsažen v XAdES je možné použít referenci.
- Důkazní materiál = soubor dokumentu + soubor XAdES.
- Ze souboru XAdES se nedovíme nic o obsahu dokumentů v něm sdružených.



# Aplikace TDPS

TRUSTED DOCUMENT PRESERVED SYSTEM

## JAK APLIKACE PRACUJE

### Aplikace TDPS - TRUSTED DOCUMENT PRESERVED SYSTEM



#### Aplikace TDPS

TRUSTED DOCUMENT PRESERVED SYSTEM

Dokument je přijat na vstupu TDPS, kde dojde ke kontrole konzistence přenesených dat a následně k provedení antivirové kontrole.

V dokumentu jsou identifikovány bezpečnostní prvky a zajištěný materiály potřebné pro ověření, které jsou nutné pro zopakování ověřovacího procesu kdykoli v budoucnu.

V pravidelných intervalech probíhá kontrola konzistence spravovaných dokumentů.

Automatické přerazítkování pomocí časových razítek.



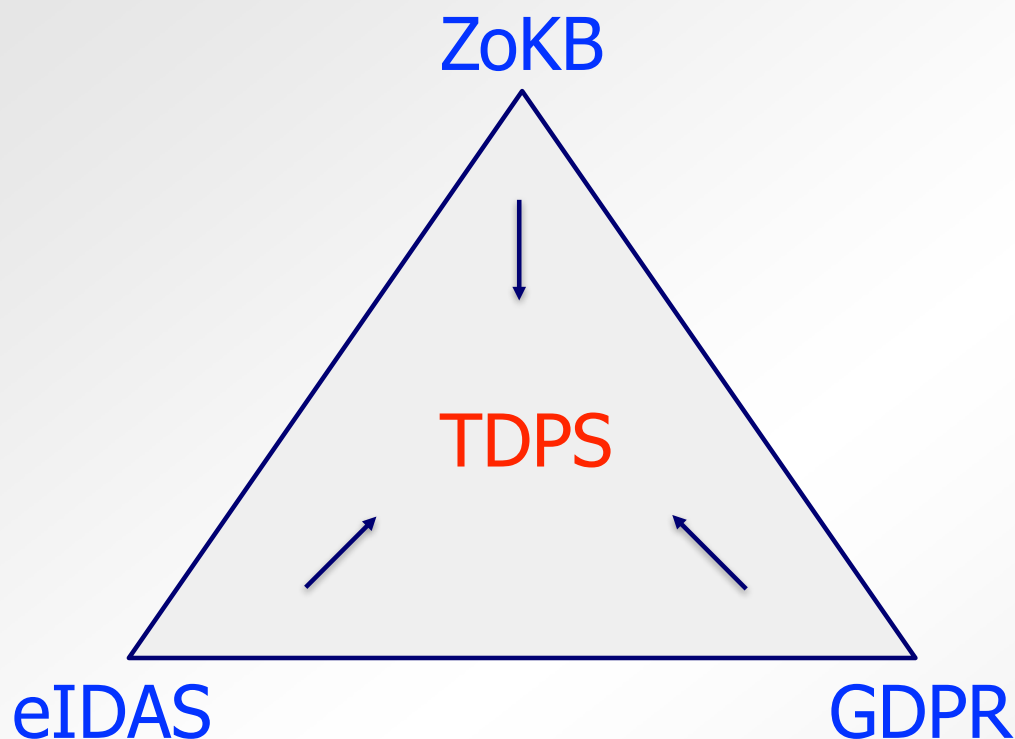
## 15 MOŽNOSTI APLIKACE

### Aplikace TDPS - TRUSTED DOCUMENT PRESERVED SYSTEM

#### DALŠÍ MOŽNOSTI APLIKACE

- ✓ Auditování událostí spojených s manipulací s elektronickým dokumentem.
- ✓ Auditování přístupu k obsahu dokumentu
- ✓ Prostředky pro znemožnění přístupu správce systému k obsahu uložených dokumentů.
- ✓ Konverze dokumentů do archivního formátu PDF/A
- ✓ Možnost vyhledávání v obsahu dokumentů

## Aplikace TDPS - TRUSTED DOCUMENT PRESERVED SYSTEM



### ZoKB

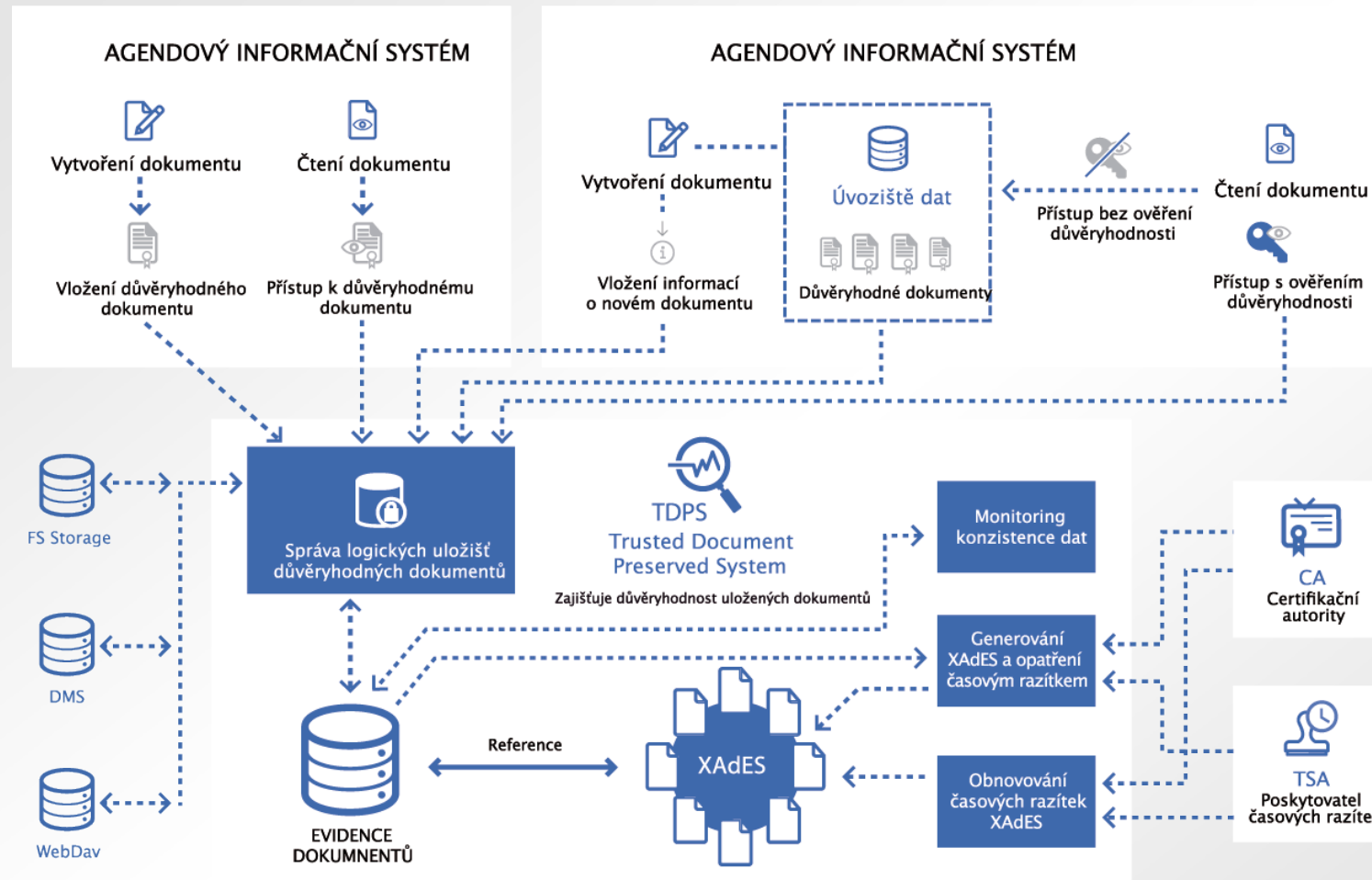
- Ochrana před škodlivým kódem
- Aktivní kontrola konzistence dokumentů

### eIDAS

- Ověření platnosti podpisu
- Uchování elektronického podpisu

### GDPR

- Ochrana před neoprávněným přístupem k obsahu
- Vyhledávání v obsahu
- Auditní stopa přístupu k obsahu



17

## Další aplikace

### ERMS - ELEKTRONICKÁ SPISOVÁ SLUŽBA

Elektronická spisová služba sloužící k evidenci papírových i elektronických dokumentů odpovídající požadavkům české legislativy o archivnictví a spisové službě

### TDPS - DUVĚRYHODNÉ

**ULOŽENÍ  
DOKUMENTŮ**  
Aplikace sloužící k zachování důvěryhodnosti všech typů elektronických dokumentů

### DIGITÁLNÍ ARCHIV

Dlouhodobé uložení digitálních i analogových dokumentů podle standardů NSESS a OAIS, s důrazem na zajištění jejich dostupnosti, čitelnosti a autenticity.